Ciencia y Tecnología

[PSA/Giga Tutorial] Como entrar a la página de Admin del Modem/ONT de GTD (2021)

OC (self.chile)

submitted 7 hours ago by JPZV [+2] Experto en cagarla

Introducción

pueden ignorar esta intro, la escribo para subir mi ego no más

De seguro aquellas personas que contrataron Fibra Óptica de GTD y que le gusta abrir puertos como yo hayan intentado entrar a `192.168.1.1`[1] o `192.168.1.254`[2] para darse cuenta de que la página está bloqueando el acceso.

Para abrir puertos al final siempre recomiendan (tanto el técnico como en foros) de poner toda la conexión en Modo Bridge, sin embargo, para mi no era una opción porque significaría que tendría que comprar Puntos de Accesos cuando el plan que tengo ya me entregaba 2 (y que para mi son mucho mejor que los que tenía antes en temas de señal).

Así que ayer me hice amigo del técnico que vino a instalar todo y me dio varios Tips para abrir el DMZ (que es lo mismo que hacía en VTR. Al final nunca entraba a su Modem sino a mi Router con DMZ), y hoy, investigando a fondo, logré descubrir una forma de vulnerar esa seguridad que pusieron, aunque no es nada fácil y que incluso puede que varios de ustedes no puedan realizar.
ahora si deben leer

Requisitos/Herramientas

- Destornillador Philips (+)
- USB-To-TTL. Son super baratos, lo pueden encontrar como a 3 lucas, no más de 10. Si no me equivoco, yo estoy ocupando el de esta publicación[3] en MercadoLibre.
- Putty[4] o cualquier cliente Serial/TTL
- Jumpers Hembra-Hembra[5] (En caso de que su USB-To-TTL no tenga)
- (Opcional) Extensor USB: Esto solo lo necesitan si los puertos USB les queda lejos.

Importante

1. Yo no me hago responsable de ningún daño, ni tampoco de alguna disputa legal que tengan. Esto lo realizan bajo su completa responsabilidad.
2. El modelo de mi ONT es el AN5506. Es posible que esto no funcione en modelos distintos.
3. Este exploit (le diré así) puede que sea *arreglado* por GTD en futuras actualizaciones. Desconozco por completo que pasará con la configuración del Router en caso de que lo *arreglen*.
4. Les recomiendo leer todo el Tutorial de pie a cabeza **ANTES** de realizar un paso, ya que cualquier paso en falso puede dejar el ONT inservible o incluso lastimarse ustedes.
5. Pueden compartir la info de este Post sin tener que preguntarme. Incluso, no necesitan dar créditos a mi persona. Entre menos gente sepa quien fue el OT, menos probable será que me atrapen con vida jeje.

1) Desconectando todo

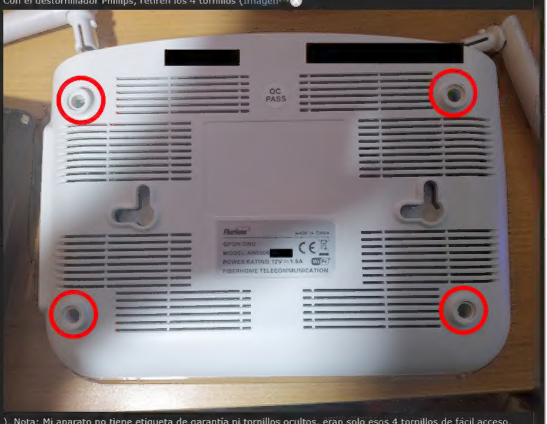
Nota: El técnico me dijo que GTD tiene un orden para sus conexiones, y al parecer para los puertos es lo mismo, asi que, cuando vayan a desconectar los cables Ethernet, pónganle una etiqueta indicando el número del puerto.

1. Vayan a donde tienen el ONT y presionen el botón para apagar. Luego, desenchufen el adaptador del ONT.
2. Desconecten **cuidadosamente** los cables de atrás siempre fijándose en los puertos en que estaban. Tengan cuidado con el cable de la Fibra Óptica, es super delicada.
3. Retiren el ONT de la cajita (en caso de que lo tengan en una pared) y pónganlo en una mesa amplia (ojalá cerca de su PC).

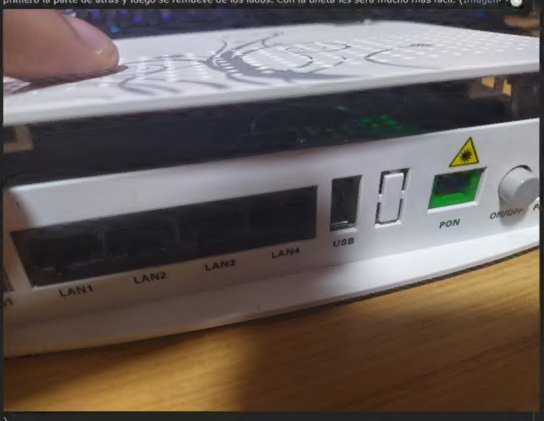
2) Desarmando

Lamentablemente para hacer este exploit hay que acceder a unos conectores internos que son imposible de acceder desde afuera.

1. Retiren las gomitas de las patitas. Son 4 gomitas en total encontradas en cada esquina.
2. Con el destornillador Phillips, retiren los 4 tornillos (Imagen[6] ⊗


[redacted] [redacted] [redacted]

). Nota: Mi aparato no tiene etiqueta de garantía ni tornillos ocultos, eran solo esos 4 tornillos de fácil acceso. Revisen de todas formas con una linterna para ver por dentro de que no tengan algún tornillo extra.
3. Den vuelta el aparato y, ocupando una *uña de guitarra* (o un kit de desarme como el de IFixIt), desanclen los clips internos que sujetan la tapa desde la parte posterior (arriba de los puertos). La tapa se abre levantando primero la parte de atrás y luego se remueve de los lados. Con la *uñeta* les será mucho más fácil. (Imagen[7] ⊗

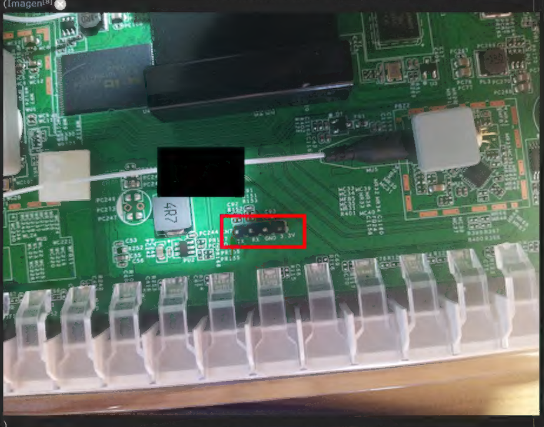


)

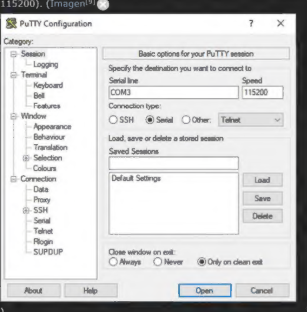
NOTA: No toquen nada de la parte interna ya que hay varias cosas delicadas y que pueden provocar un accidente de descarga eléctrica.

3) Conexión

1. Ubiquen cuidadosamente el conector UART. Este conector son 4 pines sobresalientes que están juntos. En mi caso, estaban cerca de las luces delanteras. Estos conectores tienen la etiqueta "TX, RX, GND y 3.3V" (Imagen[8] ⊗


[redacted]

)
2. Con mucho cuidado, conecten el USB-To-TTL a los pines siguiendo este esquema (El 3.3V **NO** se ocupa):
   1. USB -> ONT
      1. GND -> GND
      2. TX -> RX
      3. RX -> TX
3. Conecten el USB-To-TTL en el computador y abran el Putty (o su cliente serial). El Baud Rate del ONT es de **115200** así que deben de indicar su puerto COM (lo pueden encontrar en el Admin. de Dispositivos) y ajustar el Baud Rate a 115200 (generalmente Putty lo pone a 9600, tengan mucho ojo con eso. Cambien el 9600 a 115200). (Imagen[9] ⊗


PuTTY Configuration

Serial line: COM3

Speed: 115200

Connection type: ○ SSH ● Serial ○ Other: Telnet

Close window on exit: ○ Always ○ Never ● Only on clean exit

)
4. Conecten cuidadosamente el ONT a la corriente pero **NO** lo prendan aún.
5. Presionen en botón **Open** en Putty y esperen hasta que les salga una pantalla negra (aprovechen de ajustar el tamaño de la fuente en caso de que se vea muy pequeña).

4) El exploit

Nota: Aquí tienen que ser super atentos, rápidos y cuidadosos. Recuerden leer todos los pasos **antes** de ejecutarlos.

1. Prendan el ONT y la pantalla negra se empezará a llenar de información (imagen).
2. Lean **ATENTAMENTE** porque aparecerán dos mensajes por unos pocos segundos. El primer mensaje dice `*** Press Enter key to stop auto run (1 seconds) ***`. Ese lo deben de **IGNORAR** (es decir, **NO** presionen nada).
3. Luego, empezará a salir más información y aparecerá eventualmente este mensaje:

```
initialize.sh==

Press Ctrl + C to stop auto setup
```

Aquí es donde **deben** de presionar la tecla CTRL + C (en Windows y Linux. No estoy seguro cual es en Mac, pero creo que es Cmd + C)

1. Si lo hicieron correctamente, les debería aparecer una linea que diga algo como `/fh/extend #`, si no les aparece eso, significa que no alcanzaron, presionaron mal la tecla, o se bugueo la conexión Serial (a mi me pasó, tuve que desconectar todoy volver a conectar), en ese caso, reinicien el ONT.
2. Escriban `cat initialize.sh` y les aparecerá un montón de código. Aquí ustedes deben de copiar todo lo que hay entre `#This is the startup file of Fiberhome.` y `./runWeb.sh` (o algo parecido). Es un tremendo código que puede que varíe un poco entre ONT, así que no lo pondré aquí. El `./runWeb.sh` **NO** se copia. En Putty solo deben de seleccionar todo y no presionar nada. Luego, peguen el contenido en algún lugar (como en Notepad++).
3. Ahora deben de pegar lo que copiaron en el paso 5 de vuelta a la ventana negra (consola para los entendidos). En Putty es sencillo, solo presionan el Botón Derecho del Mouse (al menos en Windows). Recuerden **NO** copiar/pegar el `./runWeb.sh`.
4. Esperen un rato hasta que **deje** de aparecer nuevos textos en la pantalla (en algún momento va a parar).
5. Ahora, escriban estos comandos (uno por línea). Si están en putty, pueden seleccionar todo y presionar Mouse Derecho seguido por Enter.

   iptables -P INPUT ACCEPT iptables -P FORWARD ACCEPT iptables -P OUTPUT ACCEPT iptables -t nat -F iptables -t mangle -F iptables -F iptables -X
6. Finalmente, para nuestro último paso del Exploit, deben de escribir esta línea:

   ./webs -L 999 -M 1 -S 100 -m all &

Les aparecerá más texto nuevo pero no se preocupen. Solo minimicen la ventana de Putty (no la cierren).

5. A meter mano

Finalmente, el último paso es meter mano, para eso:

1. Conecten un computador (puede ser el mismo que el de Putty u otro. Yo preferí otro para evitar duplicados de IP) por Ethernet al ONT. Yo ocupé el puerto 1 porque el técnico me dijo que GTD suelen ocupar ese para configurar.
2. Recuerden poner la configuración de IP en automático en el computador (se supone que debería estar corriendo el DHCP, por lo que se les debería asignar una IP), y luego entren a la puerta de enlace predeterminada desde el navegador (si no conocen esta puerta, pueden abrir un CMD en Windows y escribir `ipconfig /all` o ver el estado del adaptador de Red). En mi caso era `192.168.1.254`
3. Les va a preguntar por una cuenta. Este al parecer nunca lo modificaron asi que debería ser `admin` como usuario, y `G0R2U1P2ag` como contraseña.
4. Metan toda la mano que quieran. Como Tip, el DMZ se encuentra en la pestaña "Applications". Sin embargo, tengan cuidado porque algunos datos lo manejan GTD y puede que dejen sin conexión la casa o los pillen. Yo solo recomiendo cambiar el DMZ y nada más.

Nota: Es probable que en Putty salgan varios errores, como diciendo que no se pudo guardar el DMZ. No se porqué aparecen esos, pero el DMZ a mi si se me activó correctamente. Recuerden anotar la IP del DMZ, porque luego de esto no podrán volver a acceder a la página sin tener que hacer todo esto de nuevo.

6. Aquí no pasó nada

1. Una vez modificado todo, reinicien el ONT. Para eso vayan a Putty y escriban `reboot`. Luego, esperen unos 3 minutos hasta que deje de aparecer texto (**NO** presionen nada esta vez).
2. Apaguen el ONT, desconecten el USB-To-TTL tanto del PC como del ONT, armen el aparato, y vuelvan a ponerlo donde estaba.
3. Prendan el ONT y esperen hasta que agarre señal de GTD, luego, hagan las pruebas que quieran para comprobar los cambios.

Preguntas Frecuentes

P: ¿Puedo hacer todo esto sin desarmar el ONT o sin comprar ninguna cosa?

R: Por lo que pude averiguar, no. GTD Actualizó el ONT bloqueando el acceso a **todos** los puertos excepto el 8099 y el 4433, sin embargo, no pude encontrar la forma en como utilizar dichos puertos.

P: ¿Hay alguna forma para dejar la página de configuración habilitada para siempre?

R: Posiblemente, ya que con este Exploit puedes acceder a cosas que incluso la misma página no te deja. Sin embargo, yo no pude encontrar la forma de hacerlo, ni tampoco quise indagar más porque un paso en falso podría dejar el equipo inservible (y me costó harto conseguir que pongan GTD aquí).

P: ¿Puedo cambiar el Firmware del ONT?

R: Posiblemente, pero posiblemente no te puedas volver a conectar a la red de GTD (la opción de actualizar al parecer está habilitada en la misma página incluso).

P: ¿Puedo abrir puertos en vez de poner un DMZ?

R: Si. No lo probé, pero debería funcionar. Eso si, ten en cuenta que cada vez que tengas que agregar, modificar, o eliminar un puerto, deberás hacer tooooooooooodo este tutorial, por eso recomiendo el DMZ.

P: ¿Qué chucha es un DMZ?

R: Para no hacerme un testamento gigante, el DMZ es técnicamente dejar todos los puertos abiertos a una sola dirección IP. Yo lo que hago es dejar el Modem/ONT del proveedor activado como está (y que dé su propia red WiFi), y, aparte, poner un Router propio con el DMZ para conexiones avanzadas/desarrollo/de trabajo y así manejar yo los puertos sin interferir con la red del proveedor (y, en este caso, sin tener que desarmar a cada rato).

P: ¿Sirve esto para otros proveedores de internet como Movistar/VTR/Claro? / ¿Sirve esto para el modelo X del ONT?

R: Lo más probable es que no. En primera nosotros ocupamos el UART, que en varios casos pueden que ni si quiera estén disponible para nosotros aún desarmando (de hecho, tuve suerte de no tener que soldar, y al parecer es algo del modelo que venga listo). En segunda, nosotros le dimos vuelta a la restricción que pusieron en la misma GTD, y puede que en otros proveedores o incluso en otros ONT no hayan hecho lo mismo.

P: No me resulta hacer X paso

R: Revisa que hayas hecho **todos** los pasos anteriores (este tutorial está escrito de forma cronológica). Si te saltaste uno o te metiste en el lugar equivocado, no podrás seguir con el tutorial. También ten en cuenta que este tutorial se escribió el 27/05/2021 y es probable que GTD parche este exploit en un futuro (ya sea con una actualización, nuevos modelos o algo aun peor). Si tienes dudas o te quedaste pegado, revisa los comentarios, a lo mejor alguien más estuvo en las mismas. Y si no encuentras nada, escribe un comentario (aunque dejo en claro que **no** volveré a desarmar el ONT. A mi me lo dejaron en un lugar de muy difícil acceso)

P: ¿Vas a actualizar la guía? / ¿Agregarás nuevos métodos más fáciles?

R: Lo más probable es que no. Mi ONT lo dejaron en un lugar muy difícil de acceder, y tampoco quiero romperlo. En el caso en que yo pierda el DMZ por alguna razón y vea que parchearon el Exploit, **puede** que me meta a indagar a ver si encuentro algún nuevo Exploit (en caso de que nadie lo haya descubierto), pero en mi experiencia con VTR (mi antiguo proveedor), y por lo que me dijo el propio técnico de GTD, es muy poco probable de que GTD se de cuenta de lo que yo hice en **mi** ONT y me desactive el DMZ.